CLAIMS

What is claimed is:

1. A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein the first electronic message is based on IPsec and is associated with a first identifier;

generating a value based on the first identifier;

sending the first electronic message to a second node;

receiving a second electronic message from the second node, wherein the second electronic message is based on IPsec and is associated with a second identifier that is different than the first identifier, wherein the second identifier is generated based on the first identifier;

determining whether the second electronic message is directed to the first node based on the value and the second identifier; and

sending the second electronic message to the first node when the second electronic message is determined to be directed to the first node.

2. A method as recited in claim 1, further comprising the steps of:

receiving a third electronic message from a third node, wherein the third electronic message is based on IPsec and is associated with a third identifier;

generating an additional value based on the third identifier;

sending the third electronic message to the second node;

wherein the step of receiving comprises receiving, after sending the first electronic message and the third electronic message to the second node, the second electronic message from the second node, wherein the second electronic message is based on IPsec and is associated with the second identifier that is different than the first identifier and the third identifier;

determining whether the second electronic message is directed to the third node based on the additional value and the second identifier; and

Docket No. 50325-0616

when the second electronic message is determined to be directed to the third node, sending the second electronic message to the third node.

3. A method as recited in claim 1, wherein the step of generating the value comprises the step of generating the value based on the first identifier and a specified scheme, and wherein the second identifier is generated based on the first identifier and the specified scheme.

4. A method as recited in claim 3, wherein the specified scheme produces a fixed length output.

5. A method as recited in claim 3, wherein the specified scheme is a hash algorithm.

6. A method as recited in claim 5, wherein the hash algorithm is a Message Digest 5 one-way hash function.

7. A method as recited in claim 1, wherein the value is a hash value, and wherein the second identifier is the hash value.

8. A method as recited in claim 1, wherein the value is a hash value, and wherein the second identifier is based at least in part on the hash value.

9. A method as recited in claim 8, wherein the hash value is comprised of a first plurality of bytes, wherein the second identifier is comprised of a second plurality of bytes, and wherein a last pair of bytes of the second plurality of bytes is a first pair of bytes of the first plurality of bytes, and wherein the step of determining whether the second electronic message is directed to the first node comprises the step of comparing the last pair of bytes of the second identifier to the first pair of bytes of the hash value.

10. A method as recited in claim 1, wherein the first identifier is a first IPsec security parameter index and the second identifier is a second IPsec security parameter index.

11. A method as recited in claim 1, wherein the first electronic message is based on IPsec tunnel mode and the second electronic message is based on IPsec tunnel mode.

12. A method as recited in claim 1, wherein the first electronic message is based on IPsec Encapsulation Security Payload (ESP) and the second electronic message is based on IPsec ESP.

13. A method as recited in claim 1, wherein the first node is an IPsec originator node and the second node is an IPsec responder node.

14. A method as recited in claim 1, further comprising the steps of creating and storing a mapping between the value and the first identifier.

15. A method as recited in claim 14, wherein the step of creating and storing comprises the steps of:
creating an association between the value and the first identifier; and
storing the association in a translation table.

16. A method as recited in claim 1, further comprising the steps of:
when the second electronic message is determined to be directed to the first node,
creating an association between the first identifier and the second identifier; and
storing the association in a table.

17. A method as recited in claim 16, further comprising the steps of:
receiving a third electronic message from the second node, wherein the third electronic message is based on IPsec and is associated with the second identifier; and
determining that the third electronic message is directed to the first node based on the association.

18. A method as recited in claim 1, further comprising the steps of:
receiving a third electronic from the second node, wherein the third electronic message is based on IPsec and is associated with a third identifier that is different than both the first identifier and the second identifier;

determining whether the third electronic message is directed to the first node based on the value and the third identifier; and

when the third electronic message is determined to be directed to the first node, sending the third electronic message to the first node.

19. A method as recited in claim 1, wherein the step of generating the value is performed before the step of receiving the second electronic message.

20. A method as recited in claim 1, wherein the step of generating the value is performed after the step of receiving the second electronic message.

21. A method as recited in claim 1, wherein the device employs network address translation (NAT).

22. A method as recited in claim 1, wherein the device employs dynamic address NAT.

23. A method as recited in claim 1, wherein the device employs network address port translation (NAPT).

24. A method for facilitating Internet security protocol (IPsec) based communications through a device that employs address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first node, wherein the first electronic message is based on IPsec and is associated with a first identifier, wherein the first identifier is generated based on a second identifier and the first identifier is different than the second identifier;

sending the first electronic message to a second node;

receiving a second electronic message from the second node, wherein the second electronic message is based on IPsec and is associated with the second identifier;

generating a value based on the second identifier;

determining whether the second electronic message is directed to the first node based on the value and the first identifier; and

sending the second electronic message to the first node when the second electronic message is determined to be directed to the first node.

25. A method for facilitating Internet security protocol (IPsec) based communications with a device that employs address translation in a telecommunications network, the method comprising the steps of:

generating a value based on a first identifier that is associated with a first node;

generating a second identifier based on the value;

receiving, from the device that employs address translation, a first electronic message that originates from the first node, wherein the first electronic message is based on IPsec and is associated with the first identifier;

in response to receiving the first electronic message, generating a second electronic message to the first node, wherein the second electronic message is based on IPsec and is associated with the second identifier;

sending the second electronic message to the device that employs address translation;

wherein the device determines whether the second electronic message is directed to the first node based on the second identifier and an additional value based on the first identifier; and

wherein the device sends the second electronic message to the first node when the device determines that the second electronic message is directed to the first node.

26. A method as recited in claim 25, wherein the step of generating the second identifier comprises the step of generating the second identifier based on the value and a third identifier.

27. A method as recited in claim 25, wherein the step of generating the value comprises the step of generating the value based on the first identifier and a specified scheme.

28. A method as recited in claim 27, wherein the value is a hash value, the first identifier is a first IPsec Security Parameter Index (SPI), the second identifier is a second IPsec SPI, and the step of generating the second IPsec SPI comprises the step of generating, prior to receiving the first electronic message, the second IPsec SPI based on the hash value.

29. A method as recited in claim 28, wherein the first IPsec SPI is a first randomly generated fixed length value and the step of generating the second IPsec SPI comprises the step of generating the second IPsec SPI based on at least a first portion of the hash value and a second portion of a second randomly generated fixed length value.

30. A method for facilitating Internet security protocol (IPsec) based communications through a router that employs network address translation in a telecommunications network, the method comprising the steps of:

receiving a first electronic message from a first IPsec originator node, wherein the first electronic message is secured using IPsec and is associated with a first security parameter index (SPI);

generating a first hash value based on the first SPI and a hash algorithm;

sending the first electronic message to an IPsec responder node;

receiving a second electronic message from a second IPsec originator node, wherein the second electronic message is secured using IPsec and is associated with a second SPI;

generating a second hash value based on the second SPI and the hash algorithm;

sending the second electronic message to the IPsec responder node;

after sending the first electronic message and the second electronic message to the IPsec responder node, receiving a third electronic message from the IPsec responder node, wherein the third electronic message is secured using IPsec and is associated with a third SPI that is different than the first SPI and the second SPI, wherein the third SPI is generated by the IPsec responder node based at least in part on the hash algorithm;

determining whether the third electronic message is directed to the first IPsec originator node based on the first hash value and the third SPI;

when the third electronic message is determined to be directed to the first IPsec originator node, sending the third electronic message to the first IPsec originator node;

determining whether the third electronic message is directed to the second IPsec originator node based on the second hash value and the third SPI; and

when the third electronic message is determined to be directed to the second IPsec originator node, sending the third electronic message to the second IPsec originator node.

31. A method as recited in claim 30, wherein the first electronic message is based on IPsec tunnel mode and IPsec Encapsulating Security Payload (ESP), the second electronic message is based on IPsec tunnel mode and IPsec ESP, and the hash algorithm is a Message Digest 5 one-way hash function.

Page 39 of 45